



Служба „Преса и  
информация“

Съд на Европейския съюз  
**ПРЕССЪОБЩЕНИЕ № 59/18**  
Люксембург, 3 май 2018 г.

Заклучение на генералния адвокат по дело C-207/16  
Ministerio Fiscal

**Генералният адвокат Saugmandsgaard Øe предлага на Съда да постанови, че дори престъпленията, които не са особено тежки, могат да оправдаят достъпа до базовите електронни съобщителни метаданни, стига този достъп да не накърнява сериозно личния живот**

В рамките на разследване на грабеж на портфейл и мобилен телефон испанската съдебна полиция отправя до съдия-следователя искане да ѝ предостави достъп до идентификационните данни на ползвателите на телефонни номера, активирани с откраднатия мобилен телефон през период от 12 дни, считано от деня на грабежа. Съдия-следователят отхвърля това искане по-специално със съображението, че деянията, довели до наказателното разследване, не представляват „тежко“ престъпление — т.е. съгласно испанското право престъпление, което се наказва с лишаване от свобода над пет години — като в Испания достъпът до идентификационните данни всъщност бил възможен само за този вид престъпления. Ministerio Fiscal (испанската прокуратура) обжалва това решение пред Audiencia Provincial de Tarragona (съд на провинция Тарагона, Испания).

Съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации<sup>1</sup> държавите членки могат да ограничат правата на гражданите, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантират националната сигурност, отбраната, обществената безопасност и превенцията, разследването, разкриването и преследването на престъпления или неразрешено използване на електронна комуникационна система.

В решения Digital Rights<sup>2</sup> и Tele2 Sverige<sup>3</sup> Съдът е използвал понятието „тежки престъпления“, за да прецени законосъобразността и пропорционалността на намеса в правото на зачитане на личния и семейния живот, както и в правото на защита на личните данни; тези две права са залегнали в Хартата на основните права на Европейския съюз.

<sup>1</sup> Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. (ОВ L 337, 2009 г., стр. 11).

<sup>2</sup> Решение от 8 април 2014 г., Digital Rights Ireland (C-293/12 и C-594/12, вж. [ПС № 54/14](#)). В това решение Съдът обявява за невалидна Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, 2006 г., стр. 54; Специално издание на български език, 2007 г., глава 13, том 53, стр. 51).

<sup>3</sup> Решение от 21 декември 2016 г., Tele2 Sverige (C-203/15 и C-698/15, вж. [ПС № 145/16](#)). В това решение Съдът постановява, че правото на Съюза *от една страна* „не допуска национална правна уредба, която за целите на борбата с престъпността предвижда общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства“, а *от друга страна* „не допуска национална правна уредба, която регламентира защитата и сигурността на данни за трафик и на данни за местонахождение, и по-специално достъпа на компетентни национални органи до запазените данни, като в рамките на борбата с престъпността не ограничава този достъп само до целите за борба с тежката престъпност, не го подчинява на предварителен контрол от юрисдикция или от независима административна структура и не изисква разглежданите данни да се запазват на територията на Съюза“.

Audiencia Provincial de Tarragona посочва, че след приемането на решението на съдия-следователя испанският законодател е въвел два алтернативни критерия за определяне на тежестта на престъплението, при която запазването и оповестяването на лични данни са разрешени. Първият е материалноправен критерий, който е свързан с терористични престъпления и престъпления, извършени в рамките на престъпна организация. Вторият е формално-нормативен критерий, който определя минимален праг от три години лишаване от свобода. Испанската юрисдикция подчертава, че този праг може да обхване огромното мнозинство от наказателни квалификации. Ето защо Audiencia Provincial de Tarragona иска от Съда да установи как се определя тежестта на престъпленията, над която накърняването на основните права може да бъде обосновано — от гледна точка на горепосочените съдебни решения — при достъпа на компетентните национални органи до лични данни, запазени от доставчиците на електронни съобщителни услуги.

В днешното си заключение генералният адвокат Henrik Saugmandsgaard Øe най-напред констатира, че мярка като поисканата от съдебната полиция в настоящия случай представлява намеса в правото на зачитане на личния и семейния живот и в правото на защита на личните данни. Според генералния адвокат обаче **в решения Digital Rights и Tele2 Съдът е установил корелативна връзка между тежестта на установената намеса и сериозността на съображението, която я обосновава.** Ето защо, за да се изисква на етапа на обосноваването на такава намеса да е налице „тежко престъпление“, което прави възможно дерогирането на принципа на поверителност на електронните съобщения, е необходимо **намесата да е сериозна. Според генералния адвокат в настоящия случай този основен елемент отсъства.**

Генералният адвокат добавя, че естеството на разглежданата по настоящото дело намеса се отличава от намесите, които са предмет на горепосочените две съдебни решения. **Мярката е целенасочена** и предназначена да предостави възможност за достъп на компетентните органи за нуждите на наказателно разследване до данни, притежавани за търговски нужди от доставчици на услуга, и обхваща единствено самоличността (лично, фамилно име и евентуално адрес) на ограничена категория абонати или ползватели на конкретно средство за комуникация, т.е. лицата, чийто телефонен номер е бил активиран от мобилния телефон, кражбата на който се разследва, **при това през ограничен период**, а именно около 12 дни. **Според генералния адвокат евентуалните вредоносни последици за лицата, за които се отнася разглежданото искане за достъп, едновременно са умерени и ясно очертани**, тъй като поисканите данни не е предвидено да бъдат оповестявани на широката общественост и възможността за достъп, с която разполагат полицейските органи, се съпътства от процесуални гаранции, понеже е свързана със съдебен контрол. **Ето защо намесата, произтичаща от предаването на тези данни за гражданското състояние, не се отличава с особена сериозност**, защото при конкретните обстоятелства такива данни не засягат пряко и интензивно интимната сфера на личния живот на съответните лица.

Генералният адвокат посочва, че съгласно Директивата дерогирането на принципа на поверителност на електронните съобщения може да се обоснове с целта от общ интерес за превенция и преследване на *престъпленията*, без по друг начин да се уточнява естеството им. Следователно не е задължително престъпленията, които легитимират разглежданата ограничителна мярка, да могат да се окачествят като „тежки“ по смисъла на решения Digital Rights и Tele2. По мнение на генералния адвокат **само когато претърпяната намеса е особено сериозна, престъпленията, които могат да обосноват такава намеса, трябва също да бъдат особено тежки. Обратно, в случай на намеса, която не е сериозна (т.е. когато данните, чието предаване се иска, не засягат сериозно личния живот), дори престъпления, които не са особено тежки, могат да обосноват такава намеса (т.е. достъпа до поисканите данни).**

Генералният адвокат приема по-специално, че **правото на Съюза допуска възможността за компетентните органи да имат достъп до държаните от доставчици на електронни съобщителни услуги данни за идентификация, позволяващи да се издирят предполагаемите извършители на престъпление, което не е тежко. Оттук генералният**

адвокат стига до извода, че в светлината на Директивата мярката, поискана от съдебната полиция в настоящия случай, води до намеса в гарантираните от Директивата и Хартата основни права, която не е толкова сериозна, че да налага такъв достъп да се предоставя само в случаите, в които съответното престъпление е тежко.

---

**ЗАБЕЛЕЖКА:** Заключение на генералния адвокат не обвързва Съда. Задачата на генералните адвокати е да предложат на Съда, при пълна независимост, правно разрешение на делото, което им е поверено. Съдиите от Съда пристъпват към разисквания по делото. Съдебното решение ще бъде постановено на по-късна дата.

**ЗАБЕЛЕЖКА:** Преюдициалното запитване позволява на юрисдикциите на държавите членки, в рамките на спор, с който са сезирани, да се обърнат към Съда с въпрос относно тълкуването на правото на Съюза или валидността на акт на Съюза. Съдът не решава националния спор. Националната юрисдикция трябва да се произнесе по делото в съответствие с решението на Съда. Това решение обвързва по същия начин останалите национални юрисдикции, когато са сезирани с подобен въпрос.

---

*Неофициален документ, предназначен за медиите, който не обвързва Съда.*

[Пълният текст](#) на заключението е публикуван на уебсайта CURIA в деня на представянето.

За допълнителна информация се свържете с **Нанчо Нанчев** ☎ (+352) 4303 4293

Кадри от обявяването на заключението са достъпни на [„Europe by Satellite“](#) ☎ (+32) 2 2964106